5/19/05

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06F 1/00, 17/60, H04L 29/06 — A1

(11) International Publication Number: WO 97/14085

(43) International Publication Date: 17 April 1997 (17.04.97)

(21) International Application Number: PCT/GB96/02489

(22) International Filing Date: 10 October 1996 (10.10.96)

(30) Priority Data:
95307148.7 10 October 1995 (10.10.95) EP
(34) Countries for which the regional or international application was filed: GB et al.

(60) Parent Application or Grant
(63) Related by Continuation
US 08/607,887 (CIP)
Filed on 27 February 1996 (27.02.96)

(71) Applicant *(for all designated States except US)*: BRITISH TELECOMMUNICATIONS PUBLIC LIMITED COMPANY [GB/GB]; 81 Newgate Street, London EC1A 7AJ (GB).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: REEDER, Anthony, Andrew [GB/GB]; 26 Parkwood, Henly Road, Ipswich, IP1 3SE (GB).

(74) Agents: MUSKER, David, Charles et al.; R.G.C. Jenkins & Co., 26 Caxton Street, London SW1H 0RJ (GB).

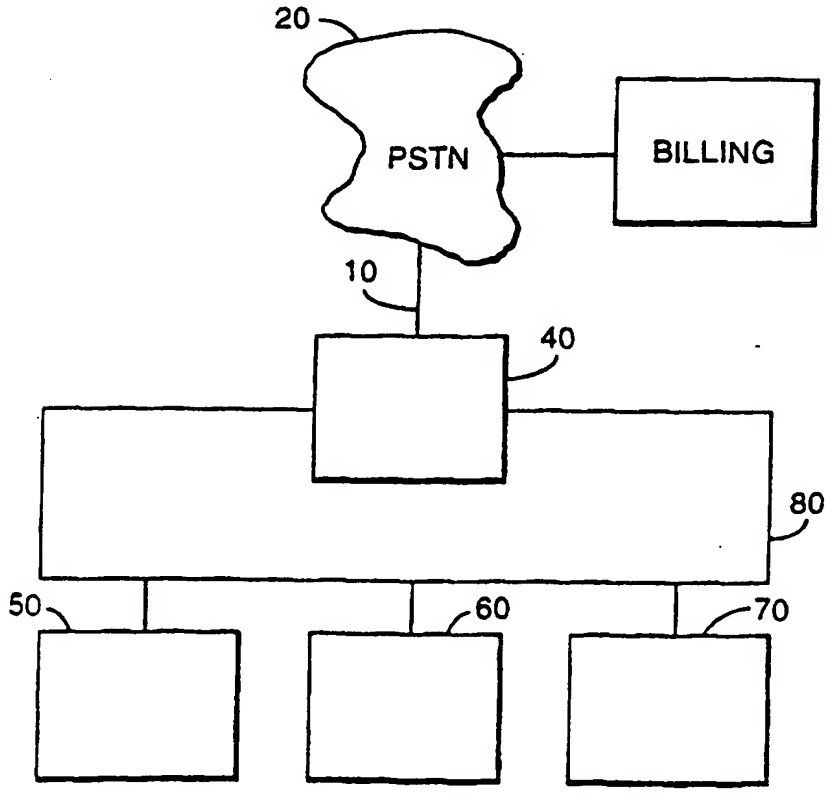
(81) Designated States: AU, CA, CN, JP, KR, NO, SE, SG, US, European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.

(54) Title: OPERATING APPARATUS WITH PAYMENT FOR USAGE

(57) Abstract

pemethod of operating apparatus for value, the apparatus being connected to a telecommunications channel, comprising the steps of: transmitting a forward message from a monitor device comprising a communications device and a programmable processor oeprating under the control of a stored program to a remote location via said telecommunications channel; receiving a corresponding return message from said remote location via said telecommunications channel; verifying said return message to determine whether it is authentic; and, if so permitting the operation of said apparatus; and, if not; inhibiting the operation of said apparatus, the program being arranged to monitor the operation of the apparatus and to perform the above steps whenever the apparatus is in use.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AM	Armenia	**GB**	United Kingdom	**MW**	Malawi
AT	Austria	**GE**	Georgia	**MX**	Mexico
AU	Australia	**GN**	Guinea	**NE**	Niger
BB	Barbados	**GR**	Greece	**NL**	Netherlands
BE	Belgium	**HU**	Hungary	**NO**	Norway
BF	Burkina Faso	**IE**	Ireland	**NZ**	New Zealand
BG	Bulgaria	**IT**	Italy	**PL**	Poland
BJ	Benin	**JP**	Japan	**PT**	Portugal
BR	Brazil	**KE**	Kenya	**RO**	Romania
BY	Belarus	**KG**	Kyrgystan	**RU**	Russian Federation
CA	Canada	**KP**	Democratic People's Republic of Korea	**SD**	Sudan
CF	Central African Republic			**SE**	Sweden
CG	Congo	**KR**	Republic of Korea	**SG**	Singapore
CH	Switzerland	**KZ**	Kazakhstan	**SI**	Slovenia
CI	Côte d'Ivoire	**LI**	Liechtenstein	**SK**	Slovakia
CM	Cameroon	**LK**	Sri Lanka	**SN**	Senegal
CN	China	**LR**	Liberia	**SZ**	Swaziland
CS	Czechoslovakia	**LT**	Lithuania	**TD**	Chad
CZ	Czech Republic	**LU**	Luxembourg	**TG**	Togo
DE	Germany	**LV**	Latvia	**TJ**	Tajikistan
DK	Denmark	**MC**	Monaco	**TT**	Trinidad and Tobago
EE	Estonia	**MD**	Republic of Moldova	**UA**	Ukraine
ES	Spain	**MG**	Madagascar	**UG**	Uganda
FI	Finland	**ML**	Mali	**US**	United States of America
FR	France	**MN**	Mongolia	**UZ**	Uzbekistan
GA	Gabon	**MR**	Mauritania	**VN**	Viet Nam

BNSDOCID: <WO_____9714085A1_I_>

OPERATING APPARATUS WITH PAYMENT FOR USAGE

The present invention relates to a method and apparatus for operating apparatus for value (for example, for rental).

Conventionally, when apparatus such as televisions or stereo equipment are hired, the charge is made for the period of time for which the apparatus is possessed by the user. This may bear no relation to the actual usage made by the user, and consequently light users may pay relatively heavy charges for the usage they make relative to heavy users.

In one aspect, the present invention provides a method and apparatus for charging for such apparatus. Essentially, a local monitor device is provided with the apparatus, without which the apparatus cannot be operated. The monitor device is connected via a telecommunications network to a remote authorisation centre, and exchanges security signals with the remote authorisation centre to permit ongoing use of the hired apparatus. The signals are transmitted whenever the apparatus is in use, and can therefore be used as a basis for charging for actual usage of the apparatus.

Thus, more flexible methods of charging for the use of computer hardware, or even for peripherals such as printers which are connected to the computer hardware, are enabled.

The same principle may be extended to other types of apparatus held at the premises of a telecommunications user provided that these contain programmable apparatus carrying a stored program (for example a microcontroller carrying an unalterable program held in read only memory to control a washing machine).

The same principle could also be applied to telemetry, in which case the controlled apparatus would be an electricity, gas, water or the like metering apparatus.

Other aspects and preferred embodiments of the invention will be apparent from the following description and claims.

Embodiments of the invention will now be described in greater detail, by way of example only, with reference to the accompanying drawings in which:

BNSDOCID: <WO_____9714085A1_I_>

Figure 1 is a block diagram showing the elements of a system for operating a programmable apparatus for value according to a first embodiment of the invention;

Figure 2a is a block diagram showing a method of downloading a control program in the embodiment of Figure 1;

Figure 2b is a flow diagram showing the operation of the programmed apparatus of the embodiment of Figure 1;

Figure 2c is a flow diagram showing the operation of a billing station in the embodiment of Figure 1;

Figure 3 is a flow diagram further showing the operation of the programmed apparatus in one example of an embodiment according to Figure 1;

Figure 4 is a block diagram showing the elements of a system for operating a programmable apparatus for value according to a second embodiment of the invention;

Figure 5 is a flow diagram modifying the operation of Figures 2b and 3 in a first example according to the second embodiment;

Figure 6 is a block diagram showing the elements of a system for operating a programmable apparatus for value according to a third embodiment of the invention;

Figure 7 is a block diagram showing the elements of a local billing device in the embodiment of Figure 6;

Figure 8 corresponds to Figure 6 and is a block diagram showing the elements of a system for operating a programmable apparatus of value according to a fourth embodiment of the invention;

Figure 9 corresponds to Figure 7 and is a block diagram showing the elements of a local billing device in the fourth embodiment of Figure 6;

Figure 10 is a signal transmission diagram showing transmission of signals in the fourth embodiment;

Figures 11a and 11b are flow diagrams showing the operation of the device of Figure 9 according to the fourth embodiment;

Figure 11c is a flow diagram showing the operation of a remote monitoring station of the fourth embodiment;

Figure 12 is a flow diagram modifying the operation of Figure 5 according to a first example of a fifth embodiment of the invention;

Figure 13 is a flow diagram modifying the operation of Figure 5 according to a second example of the fifth embodiment of the invention; and

Figure 14 is a block diagram showing the elements of a system for operating a programmed apparatus for value according to a sixth embodiment to the invention.

First Embodiment

Referring to Figure 1, in a first embodiment the present invention provides a security and billing mechanism for the use of an applications program (such as a wordprocessor) on a programmable processor apparatus (such as a personal computer or other workstation). In this embodiment, charging information is collected by one or more central charging stations, which are conveniently those used to collect telephone charging information. This embodiment is particularly concerned with charging for the use of programs downloaded via a telecommunications link.

Referring to Figure 1, a system according to this embodiment comprises apparatus 100 the use of which is to be charged; a communications link 10 linking the apparatus 100 to a telecommunications network 20 (comprising one or more switching nodes via which a plurality of other telecommunications links are accessible); a program downloading source station 30 (for example a mainframe computer coupled to the network 20 via a telecommunications link 31) and a billing station 200 (shown here as being coupled to the network 20 via a telecommunications signalling link 21).

In greater detail, the apparatus 100 comprises a communications interface 110 coupled to the telecommunications link 10 and comprising a modem and associated signalling components; a processor 120 operable under stored program control; and memory for storing the control program for the processor 120. Conveniently, and conventionally, the memory

in this embodiment may comprise a read only memory 130 which stores an operating system kernel (e.g. a machine BIOS); a random access memory 140 for storing an active control program; and a permanent memory 150 (a hard disk drive) for storing currently inactive programs and maintaining program storage during power-down of the apparatus 100.

The downloading centre 30 comprises, in greater detail, a communications interface 32 for connection to the telecommunications link 31; a store 34 for storing the program to be downloaded; and a control processor 36 for controlling the operation of the station 30.

General details of the structure of a billing station 200 are to be found in the Journal "British Telecommunications Engineering" Special Issue on Billing, vol. 11 part 4, January 1993. The components necessary for an understanding of the present invention are an interface circuit 210 for receiving and transmitting signalling data via the telecommunications channel 21; a control processor 220 (which may be provided by the mainframe billing computer); a code store 230 storing encoding and verification data; and a billing store 240 in which charging information is stored (which in this embodiment is conveniently provided by the mainframe billing stores used to record telephone charging information for use of the network 20).

The operation of this embodiment will now be explained in greater detail with reference to Figures 2 and 3.

Downloading

Figure 2a illustrates the process performed according to this embodiment when a program is downloaded. Initially, the apparatus 100 is connected, via the network 20, to the downloading centre 30 (via, for example, the Internet) under the control of a stored operating system program. On receipt of an instruction via the input device 170, the processor 120 causes the transmission by the communications interface 110 of a signal requesting the downloading of an identified program item.

In a step 1002, the downloading centre receives the

request signal transmitted by the apparatus 100. In a step 1004, a unique identifier code (comprising, for example, a lengthy binary sequence generated by a pseudo random number generator) is generated to uniquely identify this downloaded copy of the program, and the program is read from the store 34 to create a copy which is modified to insert the identifier code. In a step 1006, the unique identifier code, together with the telephone number (or other identification data) identifying the requester, are transmitted via the network 20 to the billing station 200. In a step 1008, the program (including the unique identifier code) is transmitted in serial fashion via the network 20 and links 31 and 10 to the apparatus 100, at which it is received via the communications interface and stored in the permanent store 150.

Validation

In this embodiment, the program contains code for performing the process shown in Figure 2b, which provides a validation process by each use of the program. In a step 1102, when the program is activated, prior to normal execution of the functions of the program (step 1106) in a step 1104, a validation routine is called. In the validation routine, in a step 1202, a use request signal is transmitted to the network 20. The use request signal has a format which will cause it to be directed by the network 20 to the billing station 200. For example, where the link 10 is an ISDN link comprising 2 "B" (64 kilobit per second) data channels and a "D" (16 kilobit per second) signalling channel, the use request signal comprises a data packet consisting of a header portion (indicating that this is a use request packet to be directed to the billing station 200); and a data portion (indicating the identity of the application program to be used).

Although it is not essential, it is preferred in this embodiment that the data portion should be encrypted for additional security. To ensure that the encrypted data portion differs on subsequent use request signals from the same apparatus, the data portion prior to encryption may

comprise additional, time varying, data such as the date.

In a step 1204, it is determined whether a reply has been received from the telecommunications link 10 (for example, a packet received on the D channel of an ISDN link 10 the header portion of which identifies it as a return message). In the absence of a reply, no further execution of the program is performed. It may be convenient to provide an exit from the program after a predetermined time (for example on the order of several minutes).

When a reply is received, in a step 1206 the data portion of the return message is decrypted by performing a predetermined decryption algorithm thereon, and the result is compared with the stored unique code in step 1208. If the two correspond, the processor returns in a step 1210 to execute the application program in step 1106. If the two do not correspond, in a step 1212 all further execution of the application program is ceased.

It may be convenient to provide that, after a predetermined number of invalid replies are received, the program is arranged to erase or override a portion of the copy of itself stored on the permanent store 150, or otherwise to render itself inoperable, and to indicate that this has occurred on the output device 160.

Billing

Referring to Figure 2c, the operation of the billing station 200 in this embodiment will now be described in greater detail.

On receiving a use request signal (previously transmitted in step 1202) in step 1302, the billing station 200 determined the identity of the transmitting apparatus 100; in this embodiment, for example by determining the telecommunications link 10 via which the use request signal was transmitted (using conventional calling line identification techniques). This information may also be appended to the header portion of the use request signal by the first node encountered within the network 20, for instance.

In a step 1306, the control processor 220 reads the code

data store 230 to determine whether the identity corresponds to an identity stored therein (on the basis of data previously transmitted from the downloading station 30) with a corresponding unique code word indicating a right to use the applications program. In the event that a corresponding entry is found in the code data store 230, the processor 220 is arranged to generate a reply in step 1308, by encrypting the unique code using an encryption process which can be decrypted by the decryption process performed in the apparatus 100. Preferably, the encrypted return message is arranged to vary, for each apparatus 100, over time; this may be achieved, for example by encrypting time variable data such as the date together with the unique code.

In a step 1310, the return signal thus generated is provided with a header to cause it to be routed by the network 20 to the apparatus 100 and is transmitted back to the apparatus 100.

In the event that the identity of the apparatus 100 is not found to be valid in step 1306, no return signal is generated (it would alternatively be possible to generate a predetermined invalid return signal).

In a step 1312, a charge record is recorded in the billing store 240. For example where calling line identification has been used, the record may be recorded in the entry under the identified telephone number. In this embodiment, the charge record comprises date and time information, an indication of the requested program (received in the use request signal or derived therefrom), and an indication of a unit charge for the use of that program.

Thus, the above described embodiment is operable on each occasion that an attempt is made by a user of the apparatus to use the downloaded program. On each such attempt, the identity of the user is checked (by confirming his telephone number). If the identity is not acceptable, no return signal will be sent and the program will not operate. On each occasion when a return signal is transmitted, a charge is made for the use of the program.

BNSDOCID: <WO_____9714085A1_I_>

Billing by time

Preferably, in addition to charging on each occasion when the downloaded program is used, a charge is also made based on the period of use of the program. This is achieved, as shown in Figure 3, by performing a call to point A at the start of the verification routine of Figure 2b on each occasion when a predetermined interval of time ΔT has elapsed (for example, every five minutes). Figure 3 illustrates a time test step 1108 at which the program periodically reads a real time clock (not shown) of the apparatus 100 and calls the verification routine in a step 1110 on the elapsing of the predetermined time. It may, however, be more convenient for the program to set the real time clock of the apparatus 100 to generate an interrupt after the predetermined time ΔT, and to perform step 1110 in response to the interrupt.

The operation of the billing station 200 is substantially unchanged, except that rather than recording a sequence of successive different charge entries in successive repetitions of step 1312, successive charge event signals may be generated in repetitions of step 1312, which are accumulated and recorded as a single charge entry comprising a single date and time, and a charge consisting of the product of the number of charging events thus generated and a predetermined charging rate for use of the program.

This embodiment offers some protection against fraud. Where the fraud consists of making a copy, the fraudulent user will be unable to use the copy from any other establishment, since a calling line identification technique is used which will respond only to access from the original user's correct telephone line.

Since the return signal is arranged to vary over time, it is not possible for a fraudulent user who has a copy of a program merely to tap the communications link 10 and record the return signal for subsequent simulation, nor (due to the encryption) is it possible to predict what the return signal should be on the basis of recordings of previous return signals.

It might well be possible to de-compile portions of the program, study its function and thus defeat this verification and charging mechanism of this embodiment, but the effort in so doing should deter unskilled or opportunistic fraudsters.

Rather than varying the data to be encrypted over time, it would be possible to vary parameters of the encryption process (and the corresponding decryption process). In the same manner, rather than distributing a unique code for each copy of the program, it would be possible to distribute a unique decryption algorithm in each program and a corresponding encryption algorithm to the billing station 200.

Second Embodiment

The second embodiment in general fulfils the same function as the first, and like steps and components will be given the same reference numerals and will not be described further. For convenience, several differences from the first embodiment are here described together, but it will be realised that each difference could be used with the features of the first embodiment (or other embodiments) and separately of each other. Specifically, the second embodiment differs from the first in the following respects:

1. Billing is performed at the downloading centre by the downloading entity, rather than at the billing station by the network operator.
2. Use of the program is charged by reference to use of particular functions or sub programs instead of (or in addition to) charging by time.
3. Use request messages are generated in a progressing series and, conveniently, return messages are generated by encrypting the use request messages.
4. Use is monitored over time.

Thus, referring to Figure 4, in this embodiment the downloading and distribution centre 300 comprises a downloading centre 30 substantially as described above; a use monitor store 310; and a billing device 320 comprising a billing record store 321 and a processor 322. It would, of course, be possible to provide the billing station 320 at a

separate physical location to the downloading station 30. However, conveniently, the processor 322 is in fact provided by the control unit 36 of the downloading station 30, and the signalling interface 32 serves also the billing device 320.

Validation and billing

In this embodiment, the use request signals generated by the apparatus 100 carry an address portion causing them to be routed to the telecommunications link 31, and the signalling interface 32 routes use requests to the processor 322, to be verified according to the process of Figure 2c. The apparatus 100 operates generally in accordance with Figures 2b and 3 as described above, except as modified with reference to Figure 5 below. The downloading centre 30 operates substantially as described above in relation to Figure 2a, except that in the step 1006, it is not necessary to physically send code and identification data to a separate billing station but merely to record them in the code data store 323.

Referring to Figure 5, in addition to the charge events which are generated on activation of the program (as in Figure 2b) and on elapsation of a predetermined time of operation (as in Figure 3), in this embodiment, in step 1402, on each occasion when a particular program feature, sub program or sub routine (for example, the spell check feature in a wordprocessing program) is invoked, data indicating the identity of the feature is generated in step 1404, and in step 1406, a call is executed to the sub routine commencing at point B (step 1502). The operation of the apparatus 100 in performing Figures 2b and 3 is also modified in this embodiment to call the sub routine of step 1502, rather than that of step 1202, at steps 1104 and 1110.

In step 1502, the processor 120 reads a message number M stored at a predetermined location on the permanent store 150, and in step 1504, the number is incremented and re-written to the permanent store 150.

The message number M is preferably incremented only where a valid return signal has been received.

In step 1506, a use request signal data portion is

generated by encryption of the feature number and the message number M, the encryption scrambles the data so that the encrypted data portion bears no resemblance to that generated for the previous message number M.

In step 1508, the process of the validation sub routine commencing at step 1202 of Figure 2b is executed, so as to transmit the use request message.

At the billing device 320, the process of Figure 2c is performed; in this embodiment, in the step 1304 after decryption of the use request message data portion, it is determined whether the unique code is a valid code and, if so, whether the message number M follows in sequence after the last received message number. If so, the identity is judged to be valid.

It is also determined whether the unique code corresponds to a user who is entitled to use the feature corresponding to the received feature number. For additional security, calling line identification may also be performed in this embodiment as in the first, but this is not essential.

Where the received use request message is verified as valid in step 1306, in step 1308 the return authorisation message is generated utilising the received unique code and message number, and a different encryption process to that used by the apparatus 100 in step 1506. The corresponding decryption process is utilised in step 1206, and in the event that upon decryption the unique code matches that stored within the program, the processor 120 executes a return from step 1210 to step 1510 to step 1408, and proceeds to execute the desired program feature.

Use Monitoring

On each occasion when a feature is used in this manner, a record is stored in the use monitor store 310, indicating the identity of the user and of the feature. Preferably, any further available information about the apparatus 100 is also stored. The records held in the usage monitor store 310 are periodically analysed and used in one or more of the following ways:

1. The relative usage of different features of a program is determined. This may be used in developing further improvements or modifications to the program (and such usage data may be further analysed by reference to the types of apparatus 100 using the program);
2. A long term pattern of the amount of use made by each user of the various features of the program may be built up. This may then be used to detect radical changes (when averaged over a relatively short period of time, on the order of weeks) in the use pattern of a user to detect fraudulent practices such as the use of multiple copies of the same program, or the transfer of the program to a different user (with a different use pattern).

Thus, in this embodiment, the supplier of the program is able to bill for its use, and signalling communication between the downloading centre and a separate billing station is unnecessary. It would, of course, be possible for this latter advantage to be achieved by integrating the function of the downloading station 30 into the central billing station 200 of a telecommunications network, rather than vice versa.

The use of a time varying series of use request messages prevents the fraudulent recording and reuse of a single use request message.

Furthermore, the recording of the message number on permanent storage media in the apparatus 100 ensures that even after the apparatus 100 is switched off and then switched on again the sequence is continuous. This is effective in preventing the use of multiple fraudulent copies of a program, since if two or more copies of a program are used, the message number stored in at least one of the apparatus 100 will be lower than the last message number received by the billing station 320, so that only one copy of the program will be operable.

Charging for the use of different features enables program developers to apportion royalty payments between multiple contributors to a program, as well as permitting

charging structures which accurately reflect the development costs of different parts of a program. It also makes possible the downloading of upgrades to software with a separate and additional charge for the use thereof. Furthermore, it enables program suppliers to determine the popularity or otherwise of different functions or sub programs.

Rather than using the charging events to generate a charge to the user of the apparatus, in some circumstances the user of the apparatus may have pre-paid in advance (for example by payment of a one off fee) and the charging events may be used solely to calculate payments to be made to the contributors to a program. For instance, the originator of a spell check module may be credited a certain amount on each occasion when the spell check module is used by the remote user.

In this embodiment, as in the first, a charge may be made on the basis of elapsed time. In this case, the charge may be at a different rate for different functions; thus, in invoking a function, the length of the time interval ΔT may be set in dependence upon the function. Thus, the billing station 320 may accumulate a single tariff amount for each charging event, the charging events occurring at different rates for different parts of the program.

Third Embodiment

In the third embodiment, the system of the first (or second) embodiment is varied so that historical billing information is held in a billing apparatus local to each user, in the manner of a usage meter, rather than being held centrally in a telecommunications billing station 200 or program supplier billing device 320.

Referring to Figure 6, in this embodiment, the apparatus 100 is connected via a local communications link 11 to a local billing device 400, which is connected via the line 10 and network 20 to the central billing station 200 and downloading station 30 of the first embodiment. Preferably, in this embodiment, the usage monitoring store 320 of the second embodiment is provided, in communication with the central

billing station 200.

Referring to Figure 7, each device 400 comprises a robust housing 401, and is provided with a fail to safe control system which permanently disables the device on detection of an attempt to tamper, and with tamper proof seals which make it evident when tampering has occurred.

Within the housing 401 are a local interface circuit 411 connected to the local communications link 11 and a line side interface circuit 410 connected to the telecommunications channel 10. In communication with the interfaces 411, 410 is a processor 420 (for example a microcontroller or microcomputer) operating in accordance with a stored program held in a read only memory 430. The processor 420 is connected to a display panel 460 (for example a liquid crystal display) to generate a display thereon of billing data, a printer 462, and a keypad 470 from which it is arranged to accept input instructions to control the data displayed on the display 460. Also provided in this embodiment is a local billing data store 440, which is conveniently static RAM or EPROM.

Downloading

The downloading in this embodiment is similar to that of the first embodiment, and only the differences therefrom will be explained. The local billing device 400 is generally transparent to transmissions between the apparatus 100 and the network 20, but the processor 420 is arranged to monitor all data communicated in either direction. On detecting the downloading of a program, the processor 420 creates a program record in the billing data store 440 for the downloaded program.

Validation

In this embodiment, the validation is conveniently performed as in the first embodiment. The local billing device 400 in this embodiment does not play a part in the validation process, and the processor 420 merely provides a transparent link between the interfaces 410 and 411 for the use request and authorisation messages.

Billing

In this embodiment, charge records are held locally rather than centrally. However, bills are generated centrally. Accordingly, this embodiment differs from the first embodiment in that the processor 220 of the central billing station 200 is arranged to store, for each user, a simple running total of the amount due for usage of the program, which total is incremented on each charging event.

The processor 420 of the local billing station 400 is arranged to detect each occurrence of an authorisation signal (and hence each charging event) and to log the charging events in the record created for the program in the billing data store 440 on downloading of the program as described above. Thus, the local billing device 400 keeps a complete transaction log locally. The processor 420 is arranged to accept a command from the keypad 470 to display the log, together with the associated total charge, on the display device 460, so that the user of the apparatus 100 may monitor the level of charges.

Bill Generation

Periodically (for example once a month or once a quarter) the central billing station 200 is arranged to print a bill for the total amount due stored in its record for each of the apparatus 100. The central billing station in this case is arranged to generate to all local billing apparatus 400 to cause the processor 420 thereof to print out the log stored in the local billing store 440 for the use of the apparatus 100, in the form of a statement.

Various modifications may be made to the operation of this embodiment. For example, as in our above referenced earlier European application 943089904 (agents ref A24829), a limited amount of call record data may be held in the store 240 at the central billing station and a reconciliation performed between the records held in the central billing station and the local billing stations 400.

Alternatively, rather than generating a statement locally, on receipt of a bill generation signal from the

central billing station 200, the local billing device 400 may transmit the accumulated transaction log from its billing store 440 to the central billing station (this does, however, entail a higher volume of data being transmitted through the network 20).

Since in this embodiment the total amount due is stored centrally, with only descriptive data being held locally, attempts to tamper with the local billing device 400 will not in general lead to a loss of revenue, but merely to the possibility for disagreement between the user of the apparatus and the operator of the central billing station 200.

However, nonetheless, the security of this embodiment may be increased by providing that the processor 420 is arranged to further encrypt use messages received at the interface 411 before retransmitting them on the interface 410, and to decrypt authorisation messages received at the interface before passing them on to the interface 411.

Correspondingly, the central billing station 200 is arranged to perform corresponding additional encryption and decryption stages. Thus, it is not possibly simply to bypass the local billing device 400, since the signals passing along the communications channel 10 include an additional stage of encryption relative to those passing along the local link 11.

Although the above described embodiment has been illustrated with reference to the first embodiment in which a central billing station is provided, it will be readily apparent that the local billing station could equally well communicate with the downloading centre 30 at which the validation and billing could be carried out as in the second embodiment, rather than at the central billing station 200 of the first embodiment.

Finally, instead of maintaining a running total of the amount due for the use of each apparatus 100 in a central billing store 240 (or a billing store at the downloading centre of the second embodiment) it would be possible, in this embodiment, to store all charging information locally.

In this case, at periodic intervals (for example monthly

or quarterly), or when the total charge reaches a predetermined level, the processor 420 is arranged to transmit billing data comprising at least the total due to the central station (or downloading station) for the generation of a bill. If no central record of the amount due is maintained, then the physical security (geographical location and strength of the housing 401) of the local billing device 400 is of greater importance.

Fourth Embodiment

In the above described third embodiment, the validation and authorisation stages were performed by the exchange of encoded signals between the apparatus 100 and a remote point (the central billing station 200 or downloading centre 230) via the telecommunications network 20, as in the first and second embodiments respectively, whereas some or all of the charging data was stored in the local station 400.

In this embodiment, however, the local billing device 400 is arranged to perform the validation and authorisation signalling as well as (or, in principle, instead of) maintaining local charging records.

In this embodiment, to avoid potential attempts to defraud the program supplier, by tampering with the local billing device 400, the continued operation of the local billing device 400 is continually monitored via the network 20.

Referring to Figure 8, in this embodiment, the central billing station 200 is replaced by a central monitoring station 500, which is arranged to monitor the correct functioning of the local billing device 400.

Referring to Figure 9, in this embodiment, the local billing device 400 operates generally in accordance with the third embodiment illustrated in Figure 7, but additionally includes a code store 435 (functionally corresponding to the code store 230 of the first embodiment).

Downloading

In this embodiment, as in the first embodiment a program is downloaded generally according to the process shown in

Figure 2a. However, rather than sending the unique code to the central billing station 200 of the first embodiment, it is transmitted (preferably in a preliminary transmission) to the local billing device 400, as is the program. The presence of the unique code is recognised by the processor 420. The local billing device 400 receives the unique code and stores it in the store 435. The downloaded program is transmitted onto the apparatus 100, whereas the unique code is not.

Validation

The validation process in this embodiment operates as described above in relation to the first or second embodiments, but with the processor 420 performing the function of checking the validity of the use request signal received from the apparatus 100, by reference to the code stored in the code store 435, and transmitting back an authorisation signal to permit operation of the apparatus 100, as will be described in greater detail below.

Billing

On each occasion when an authorisation signal is returned to the apparatus 100, a charging event occurs, and a corresponding record is recorded in the store 440, as in the third embodiment.

The operating condition of the local billing unit 400 is periodically monitored. In greater detail, referring to Figures 10 and 11, in a step 1650 the processor 420 checks for receipt of a use request signal at the interface 411 from the apparatus 100. If a use request signal is received, in step 1652 the processor 420 accesses the code stored for the program in the store 435, and in step 1654 it checks the validity of the use request signal.

If no signal was received in step 1650, or if an invalid signal was received (step 1654), in step 1656, the processor 420 determined whether a predetermined period of time has elapsed since a monitoring signal was last sent to the monitoring station 500. The period of time Δt may be on the order of several minutes; at any rate, it is sufficiently short that a fraudulent user cannot within the period

dismantle the local billing station 400 and circumvent the operation of the processor 420.

If the predetermined period has elapsed, then in step 1658, the processor performs the monitoring routine of Figure 11b. In a step 1660, the processor 420 performs a self-test to determine whether it is functioning correctly, and to determine whether the housing 401 is still closed. In a step 1662, the results of the self test are assessed and, if the self test indicates defective operation, in a step 1664 the process 420 sends (or attempts to sends) a failure signal by the interface 410 to the monitoring station 500, and terminates operation.

If the self test indicates no failure, in a step 1666 the processor 420 generates a condition monitoring signal which is transmitted via the interface 410 to the monitoring station 500. Preferably, the condition monitoring signal comprises encoded data selected from a non repeating sequence known both to the local billing device 400 and the condition monitoring centre 500, in the same manner as described above in the second embodiment.

Referring to Figure 11c, in steps 1750 and 1752, the central monitoring station 500 determines whether a condition monitoring signal has been received within the predetermined time Δt, and if not, then the local billing device is recorded as being faulty. If a signal has been received, in a step 1754 the monitoring station 500 determines the validity of the signal by decoding the signal and determining whether it follows in the predetermined sequence; if not, then as before the local billing device 400 is recorded as being faulty. If the received signal is valid, then an encrypted reply (based, as described above, on the received signal) is transmitted back in a step 1756.

Thus, as shown in Figure 10, periodic condition monitoring signals y_1-y_5 are transmitted from, and periodic reply signals z_1-z_5 are received by, the local billing device 400.

Referring once more to Figure 11b, in step 1670, on

receipt of the reply signal transmitted from the central monitoring station 500, in step 1668, the processor 420 is arranged to determine whether or not the reply signal is valid, by decoding the reply signal and testing whether it corresponds to the signal transmitted in step 1666. In the event that the reply signal is incorrect, an attempt to tamper with the line 10, the network 20 or the local billing device 400 is likely. Accordingly, the processor 420 performs the step 1664 as described above.

When a valid reply signal is received, the processor 420 returns to its departure point in Figure 11a.

Referring to Figure 11a, on receipt of a valid use request signal x_3-x_4, in step 1672, the processor 420 is likewise arranged to perform to the processor of Figure 11b and, in the event that a valid reply signal is received as described above, in a step 1674 the processor 420 generates an authorisation signal w_3-w_4 as in the first or second embodiments, and transmits the authorisation signal back to the apparatus 100 in a step 1676. In a step 1678, a corresponding charge event is stored in the billing record store 440.

Thus, in this embodiment, the validation process is performed locally to the apparatus 100, somewhat in the manner of a conventional dongle.

However, rather than being held in an item of hardware the property of the user, the validation information is held in a local billing station which is the property of the telecommunications operating entity operating the network 20, and which can receive new security and validation information via the network 20. Thus, on downloading an upgrade or alteration to a program, a new unique code can be supplied to the local billing device 400 so that fraudulent users who may have acquired knowledge of the previous unique code are not able to use the update. Even when no update is transmitted, the downloaded program may be arranged to periodically require a new code and the new code may periodically be transmitted from the downloading centre 30 to the local billing device

BNSDOCID: <WO_____9714085A1_I_>

400.

Furthermore, and quite unlike existing security measures, the exchange of security information is used to generate billing events (as in the first and second embodiments) which are then locally recorded.

The connection of the local billing device 400 to the telecommunications network 20 enables remote monitoring of the condition of the local billing device 400 to be performed, which thus reduces the possibility of attempts to tamper with the local billing device, by periodic self test and transmission of signals to the remote monitoring device 500. Attempts to tamper with the link 10 to defraud the local billing device 400 are defeated by the provision of return messages from the remote monitoring device 500.

As in the third embodiment, at periodic intervals (for example once a month or once a quarter) the local billing device 400 transmits a total due signal, indicating the amount of payment due, via the line 10; conveniently, in this embodiment, the signal is transmitted to the downloading station 30 (the originator of the program) which is therefore able to charge the user.

If the bill is not paid, the downloading centre 30 signals to the remote monitoring centre 500 to cease further communication with the local billing device 400, which therefore ceases to receive return messages and ceases to transmit authorising signals to the apparatus 100, preventing further use of the program until the bill is paid.

As in the third embodiment, in this embodiment the local billing device 400 is arranged to display totalised charges to the user, or to print them out, on request via the input device 470.

As in the third embodiment, the local billing device may transmit transaction details, rather than just the total due, to the downloading station 30.

In an alternative arrangement according to this embodiment, rather than accumulating billing information, the local billing device 400 may be equipped with a means for

receiving electronic payment (for example a smart card reader) and may debit a users payment device (for example smart card) on each charging event. In this case, the local billing device 400 utilises the telecommunications network 20 to perform the electronic payment signalling (according to, for example, the MONDEX (TM) payment system).

Bills can be generated either on reaching a locally met threshold or on a time basis (e.g. monthly or quarterly).

Fifth Embodiment

In the preceding embodiments, the program operating the apparatus 100 was arranged to generate an exchange of signals corresponding to charging events for use of the program. In this embodiment, on the other hand, the program is a database access or other information retrieval program (specifically, for example a Web Browser program such as World Wide Web (TM) or Mosaic (TM)), and charges are made for the use of downloaded information rather than for the use of the program.

In some cases, the price to be charged for retrieval of a file of data is known in advance. In such cases, the apparatus may follow the process of Figure 7 (which is a modification of that of Figure 5).

In Figure 7, on receipt of an instruction (step 1602) to download predetermined data, the routine of step 1502 of Figure 5 is performed. In step 1604 the arrangement of the system may be either according to Figure 1 or Figure 4. The billing device follows the process of Figure 2c, and the apparatus 100 that of Figures 2b and 5 a modified by Figure 7.

If the user is verified as being authorised to access the data, and after generating a billing event signal, in step 1606 the program proceeds to download the data.

In general, the price to be paid for use of data may not be known in advance to the program. In this case, the program is arranged to execute the process of Figure 8. In this case, downloaded data for the use of which a charge is to be made contains a file header indicating the charge, together with an indication of the identity of the data (e.g. the World Wide

Web page number). When the program downloads the data in step 1702, via the telecommunications channel 10, it is arranged in step 1704 to read the price and data identification fields, and to call the verification sub routine of step 1502 of Figure 5 in step 1706.

In executing the verification routine, the processor 100 generates the use request signal utilising the data identification and price fields, and in following the process of Figure 2c, the billing device is arranged to utilise the price to generate the charging event (e.g. to store the price in a billing record).

After the billing event, and in the event that the user is authorised to download the data, in step 1708 the apparatus proceeds to permit the user to view or otherwise process the data. If not, the apparatus erases the downloaded data.

Sixth Embodiment

This embodiment operates in general according to the first, second, third or fourth embodiments, except that the program is embodied within the operating system of the apparatus 100 rather than within an applications program. Thus, a charge is made on every occasion when the apparatus 100 is used, according to the duration of use. In this way, the rental charge for computer equipment may be levied via the billing system of the telecommunications network, in dependence upon the actual level of use of the apparatus.

Seventh Embodiment

In this embodiment, a plurality of apparatus 50, 60, 70 such as household appliances are charged on the basis of use, as in the above described sixth embodiment. For example, 50 may be a telephone set; 60 may be a video recorder; 70 may be a printer; and so on. All such devices are interconnected via a local area network 80 (which may be the electrical mains circuit if each of the devices 50-70 is equipped with a suitable modem). A head station 40 is connected to the LAN 80 and to the telecommunications channel 10. The head station 40 may comprise the local billing station 400 of the third or fourth embodiments, adapted to monitor multiple apparatus 50-

70. Alternatively, it may merely interconnect the LAN 80 and PSTN 20.

Each of the devices 50-70 comprises a microcontroller operating a stored program for executing the process of Figures 2b and 3, and/or 2b and 5. Thus, in this embodiment, multiple appliances may be charged according to the level of their use, or according to the use of special features thereof, via a communications channel, rather than being charged on a weekly or monthly basis.

In the above embodiments, the apparatus could for example comprise a utility metering device such as a master valve or electricity meter. In this case, the utility metering apparatus would include a control processor and a telecommunications link.

More specifically, in the seventh embodiment, the controlled apparatus could comprise the utility metering device and a separate local head station or monitoring device could be provided, in communication with the telecommunications channel.

It will be recognised that the above described embodiments are merely examples of the invention, and that the features of various embodiments may be used in different combinations than those described explicitly above. Moreover, the skilled reader will recognise many modifications and substitutions which may be made without departing from the present invention. Accordingly, any and all such modifications are substitutions are to be regarded as forming part of the invention. Protection is sought for any and all novel subject matter or combinations of subject matter which may be disclosed herein.

BNSDOCID: <WO_____9714085A1_I_>

CLAIMS:

1. A method of operating apparatus for value, the apparatus being connected to a telecommunications channel, comprising the steps of:

transmitting a forward message from a monitor device comprising a communications device and a programmable processor operating under the control of a stored program to a remote location via said telecommunications channel;

receiving a corresponding return message from said remote location via said telecommunications channel;

verifying said return message to determine whether it is authentic; and, if so;

permitting the operation of said apparatus; and, if not;

inhibiting the operation of said apparatus, the program being arranged to monitor the operation of the apparatus and to perform the above steps whenever the apparatus is in use.

2. A method of charging for the operation of apparatus comprising the steps of;

receiving a forward message from a monitor device associated with the apparatus;

verifying said forward message to determine whether it corresponds to a predetermined said apparatus; and, if so;

transmitting a return message to said monitor device; and

generating a charging event associated with said use of said apparatus.

3. A method according to claim 2, in which the apparatus is connected to a telecommunications channel via which said forward and return messages are carried.

4. A method according to any preceding claim, in which there is provided a predetermined progressive sequence of differing said forward messages.

5. A method according to any preceding claim, in which

said forward message comprises an encoding of predetermined forward message data.

6. A method according to any preceding claim, in which said return message comprises an encoding of predetermined return message data.

7. A method according to claim 6 when appended to claim 4, in which said predetermined data comprises said forward message data.

8. A method according to claim 3, in which said step of verifying comprises a step of identifying the telecommunications channel, and a step of comparing the identity thus determined with that associated with said apparatus.

9. A method according to claim 2 or any of claims 3 to 8 appended thereto, further comprising the step of recording said charge in a stored record associated with said apparatus.

10. A method according to claim 9 appended to claim 3, in which said stored record is associated with the telecommunications channel associated with said apparatus.

11. A method according to claim 9 in which said stored record is stored at a distributed site associated with the apparatus.

12. A method according to claim 2 or any of claims 3 to 8 appended thereto, further comprising the step of generating a debit signal to an electronic payment means.

13. A method according to claim 12, in which the electronic payment means is a payment card.

14. A method according to claim 12 or claim 13, further

BNSDOCID: <WO_____9714085A1_I_>

comprising the step of inhibiting the operation of said apparatus in the absence of a payment corresponding to said debit signal.

15. A method according to any preceding claim, in which the forward messages are generated at predetermined time intervals whilst the apparatus is in use.

16. A method of operating apparatus for value, the apparatus being connected to a telecommunications channel, comprising the steps of:

transmitting a forward message from said apparatus to a remote location via said telecommunications channel;

receiving a corresponding return message from said remote location via said telecommunications channel;

verifying said return message to determine whether it is authentic; and, if so;

permitting the operation of said apparatus; and, if not;

inhibiting the operation of said apparatus.

17. A method of charging for the operation of apparatus comprising the steps of;

receiving a forward message from said apparatus;

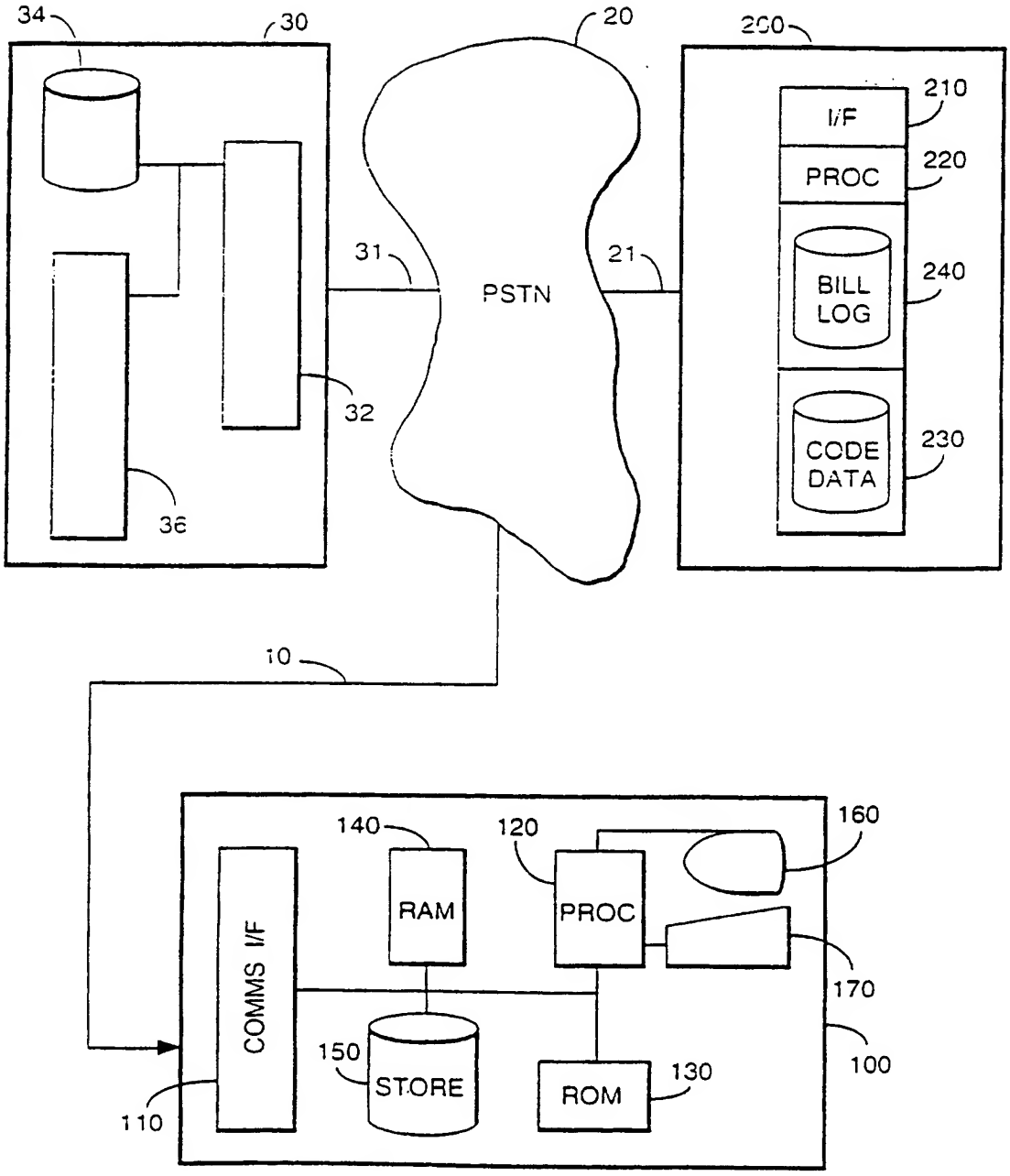
verifying said forward message to determine whether it corresponds to a predetermined said apparatus; and, if so;

transmitting a return message to said apparatus; and

generating a charging event associated with said use of said apparatus.

BNSDOCID: <WO_____9714085A1_I_>

Fig.1.



BNSDOCID: <WO_____9714085A1_I_>

Fig.2a.

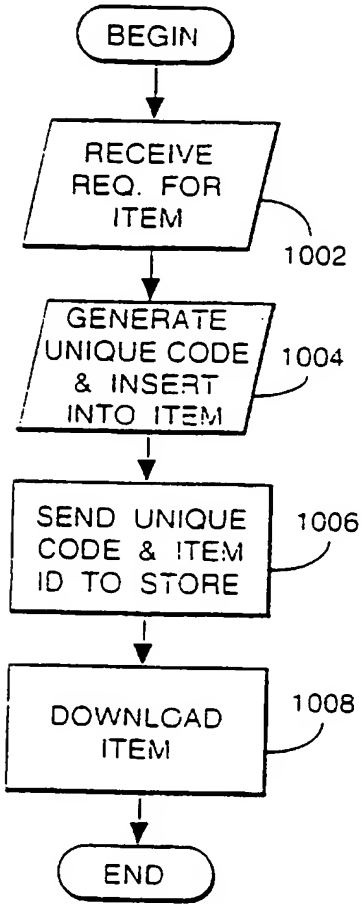


Fig.2c.

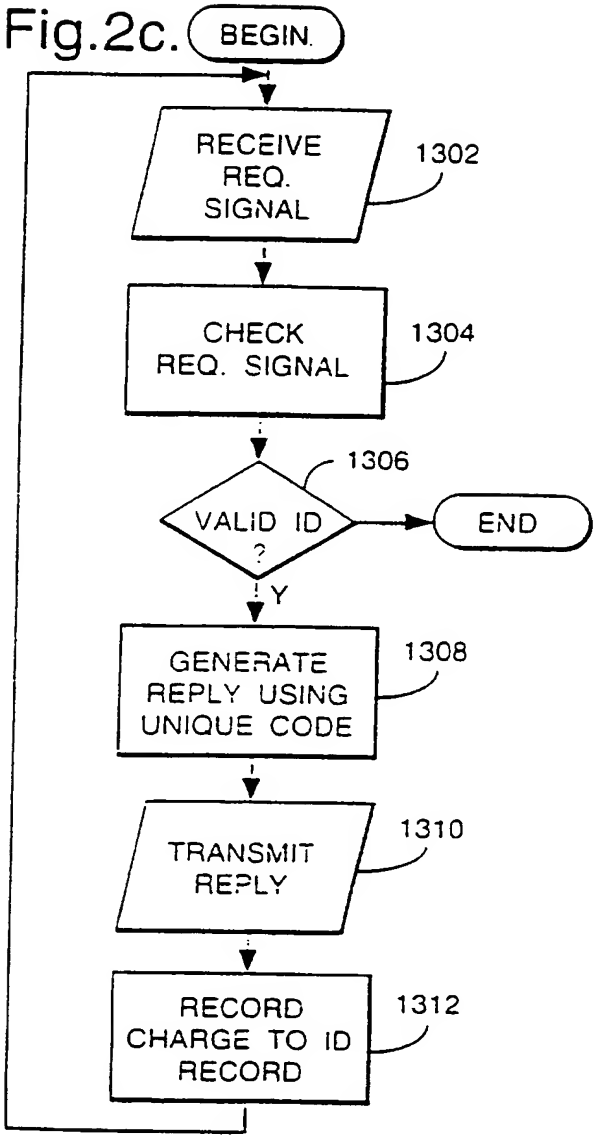
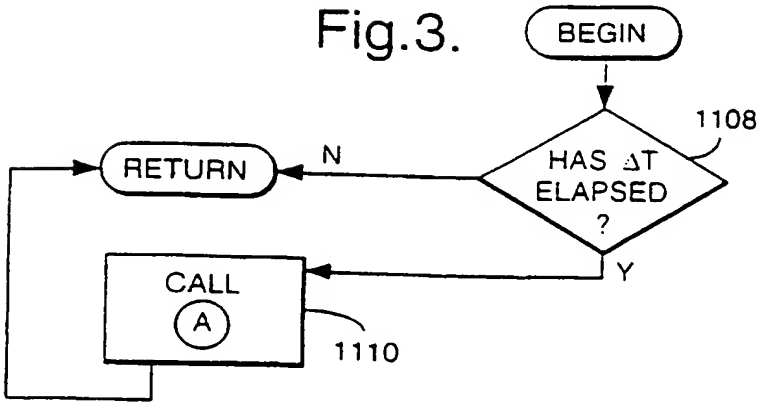
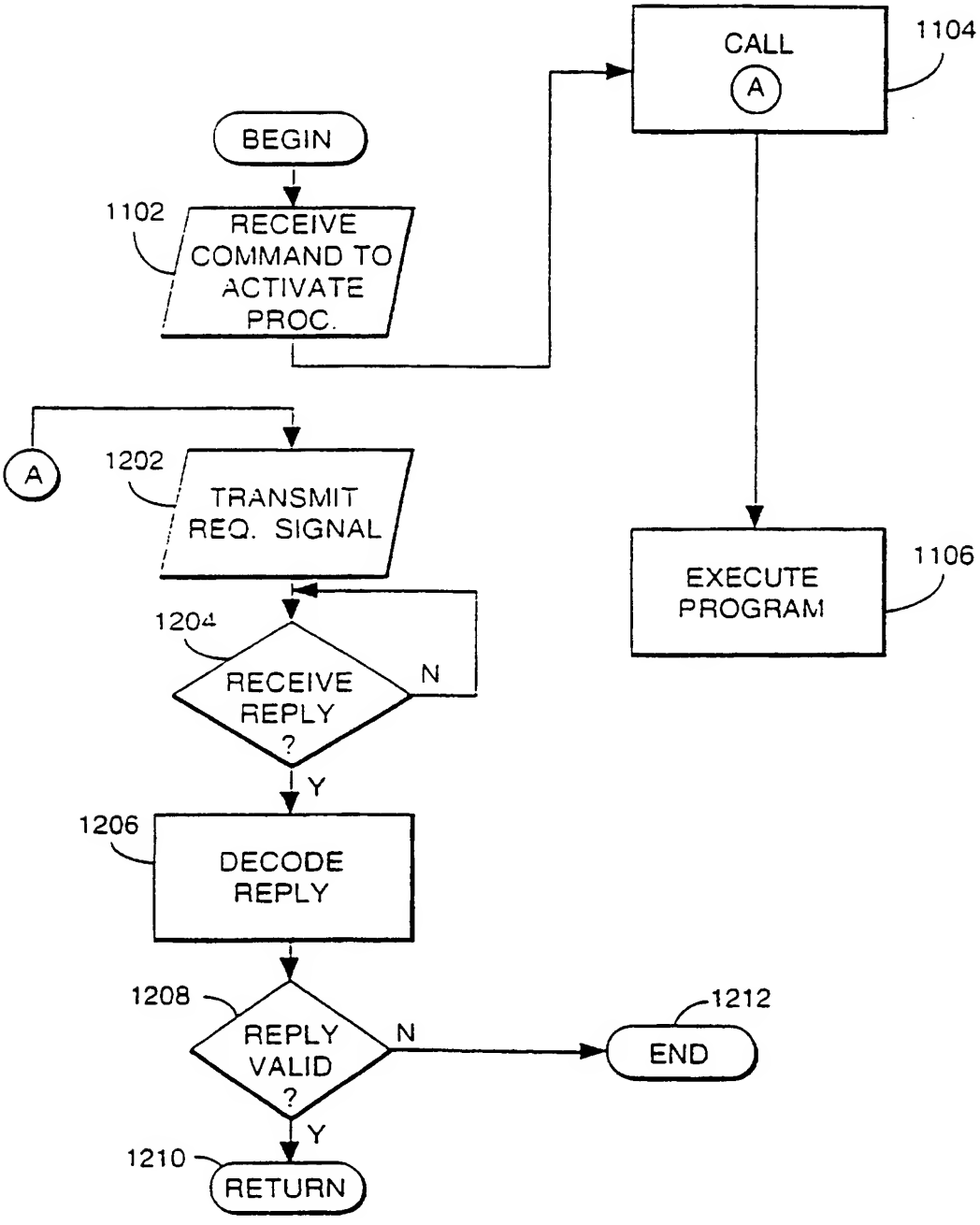


Fig.3.



BNSDOCID: <WO_____9714085A1_I_>

Fig.2b.



BNSDOCID: <WO_____9714085A1_I_>

Fig.4.

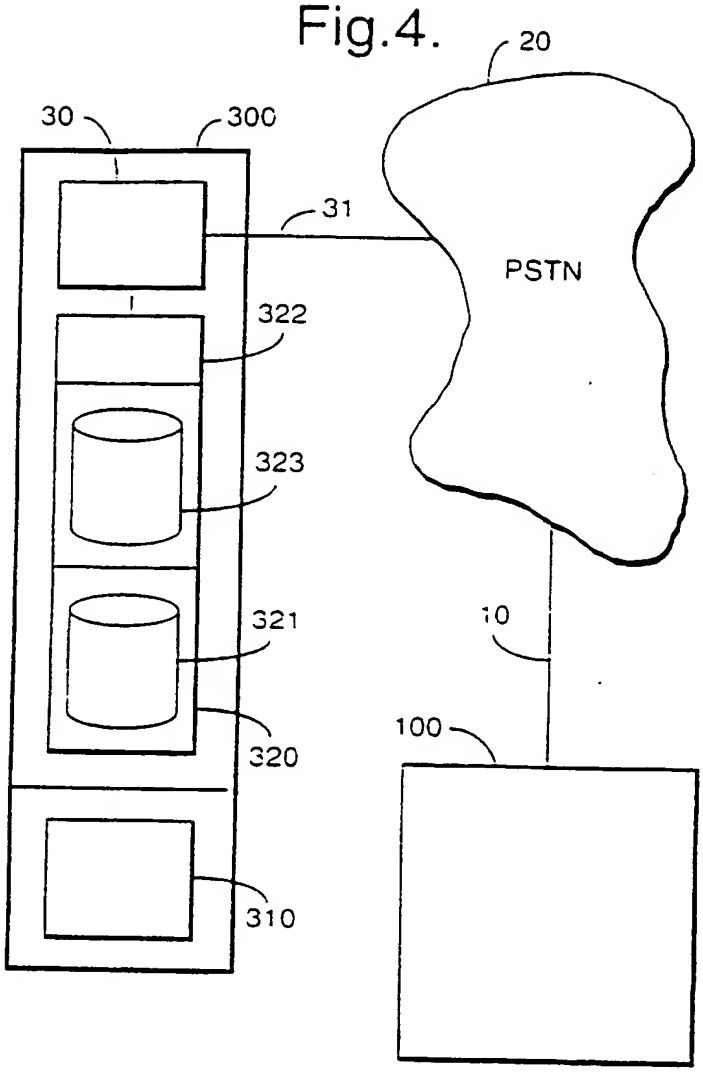
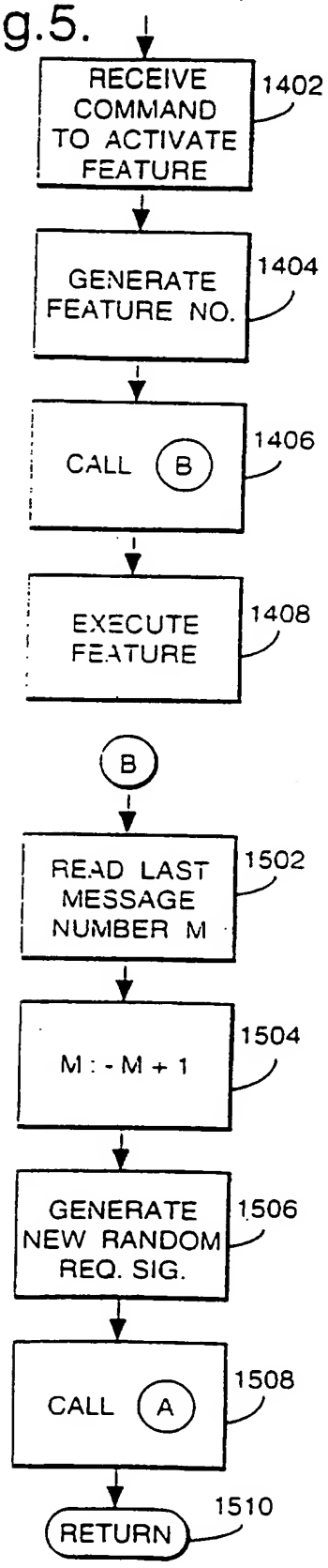


Fig.5.



BNSDOCID: <WO_____9714085A1_I_>

Fig.6.

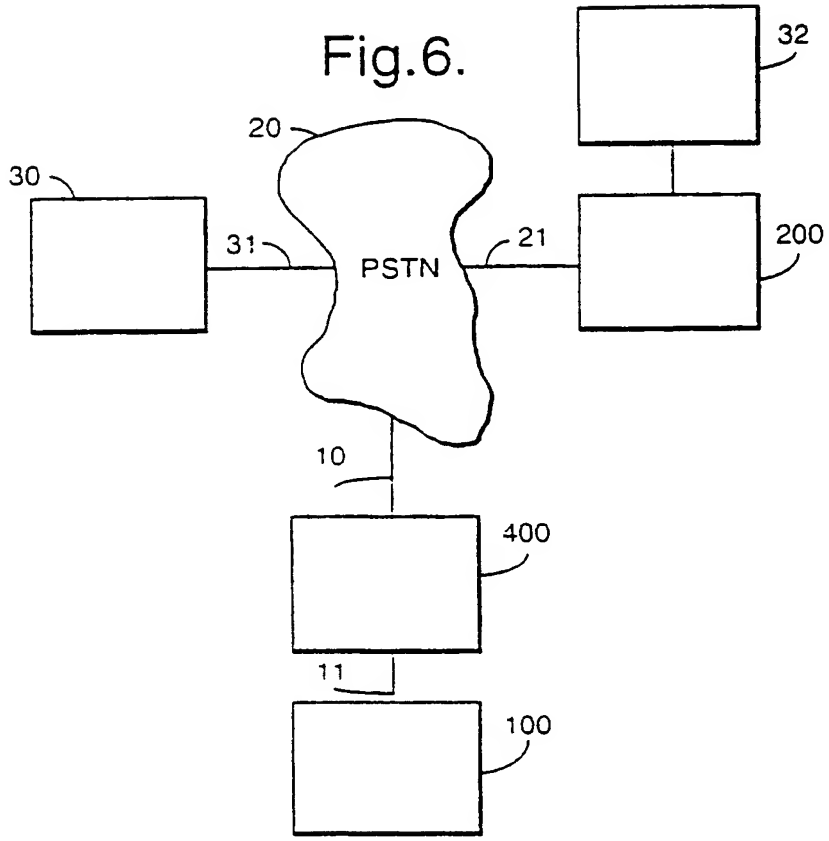
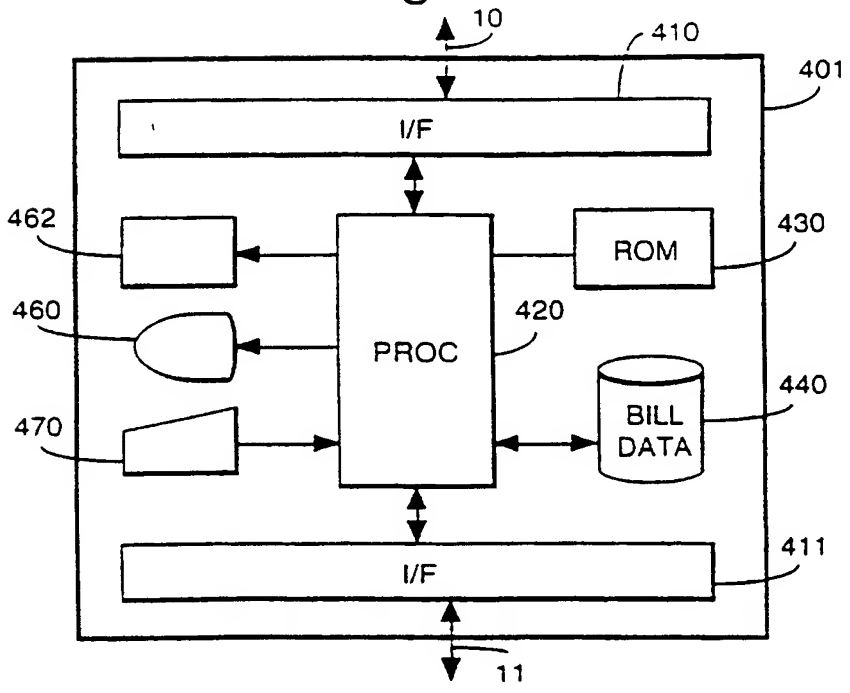


Fig.7.



BNSDOCID: <WO_____9714085A1_I_>

Fig.8.

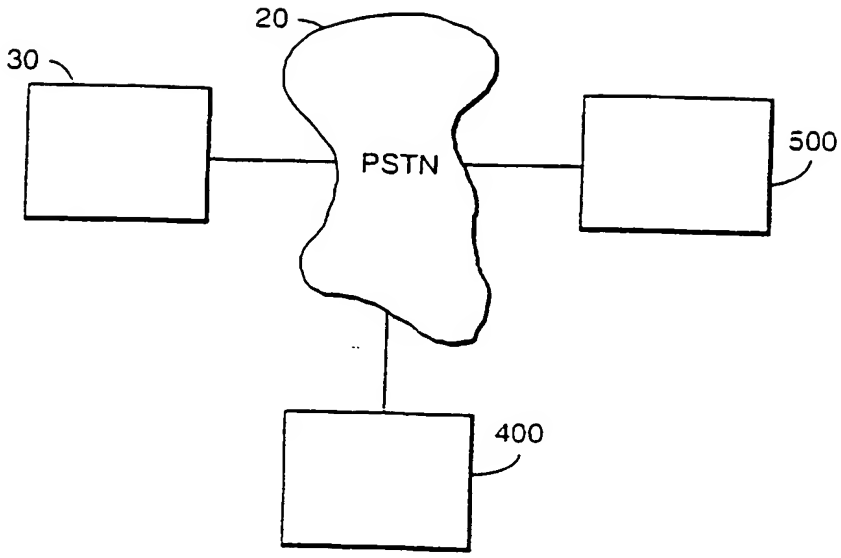
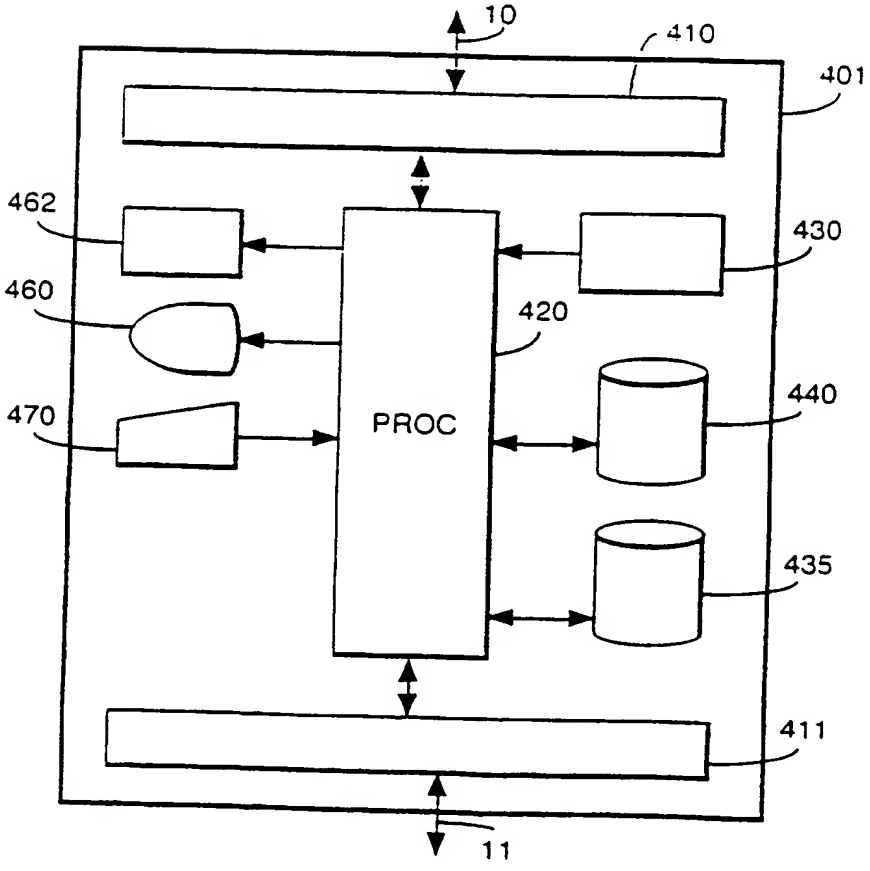


Fig.9.



BNSDOCID: <WO_____9714085A1_I_>

Fig.10.

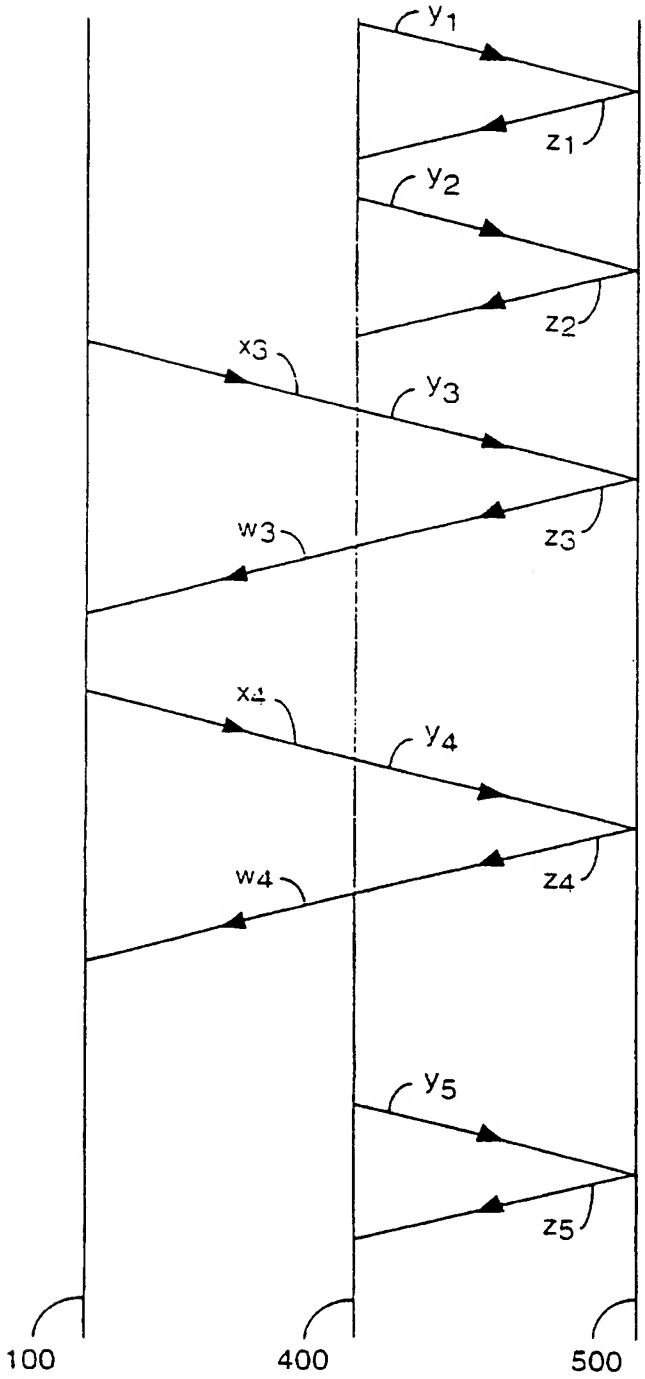


Fig.12.

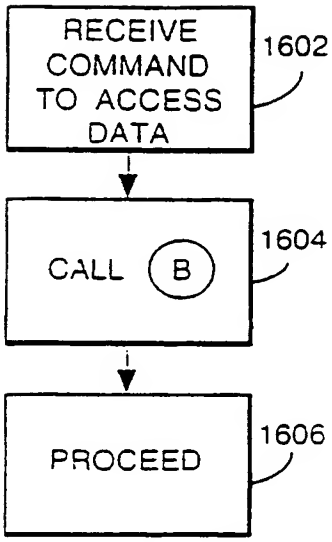
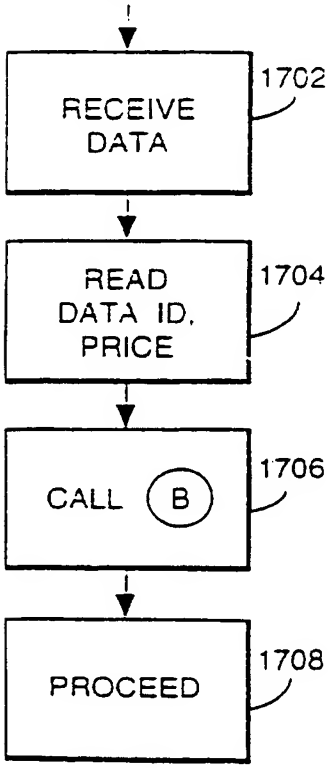
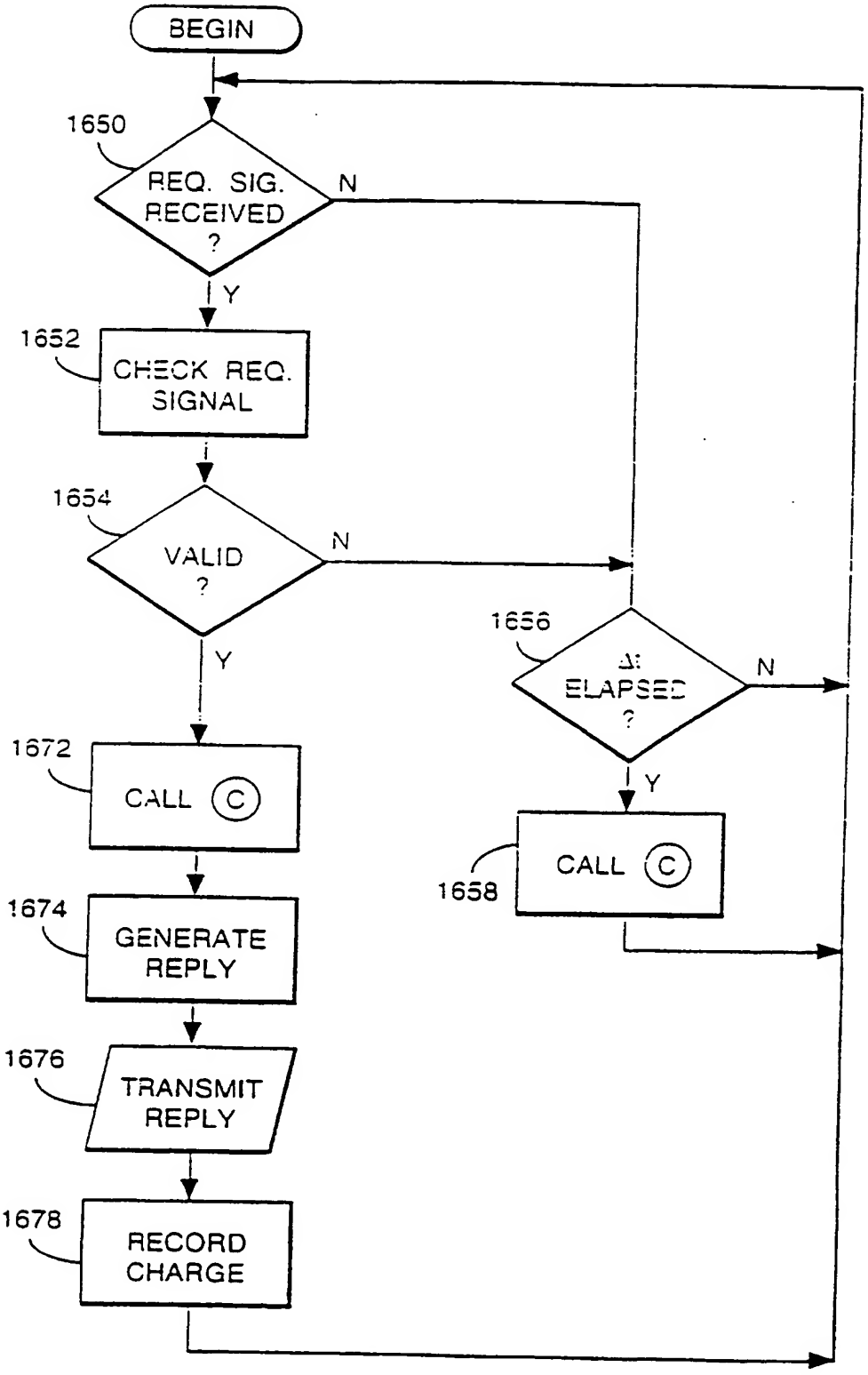


Fig.13.



BNSDOCID: <WO_____9714085A1_I_>

Fig.11a.



BNSDOCID: <WO_____9714085A1_I_>

Fig.11b.

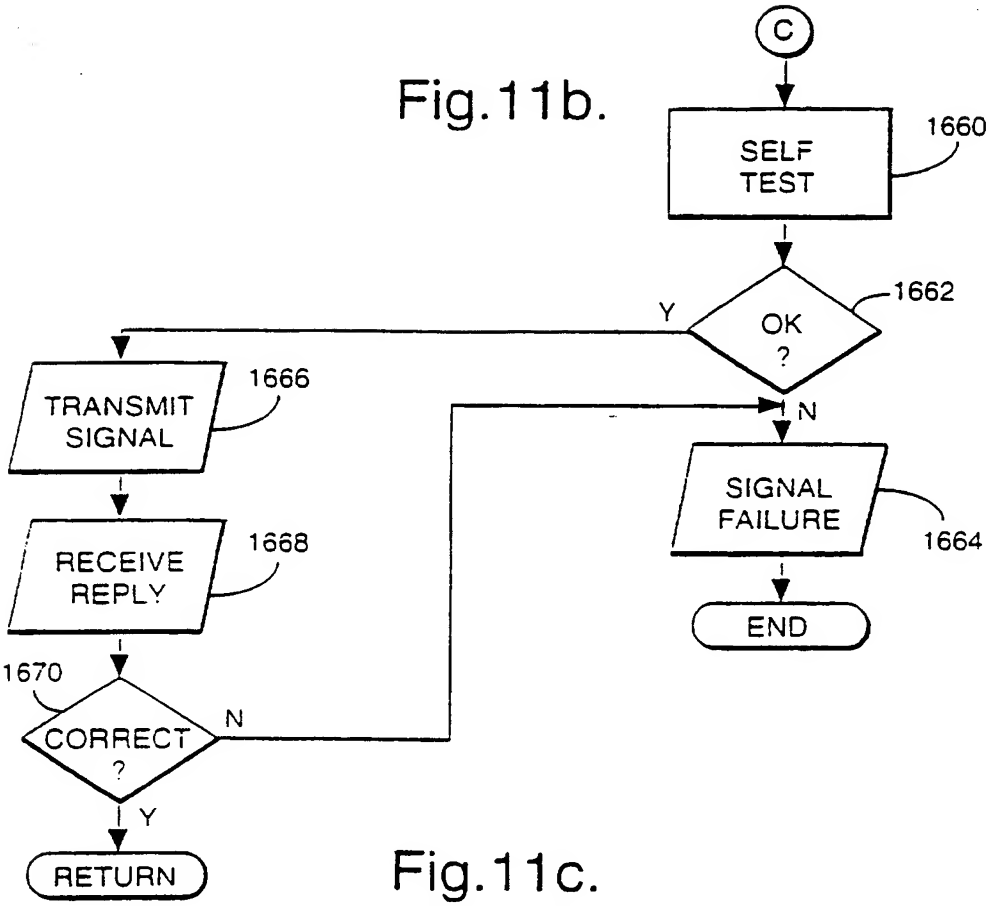
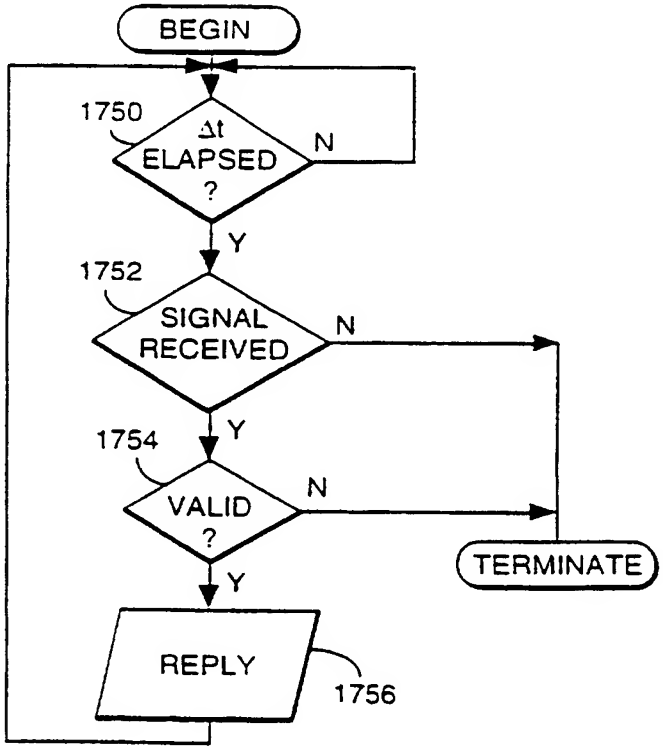
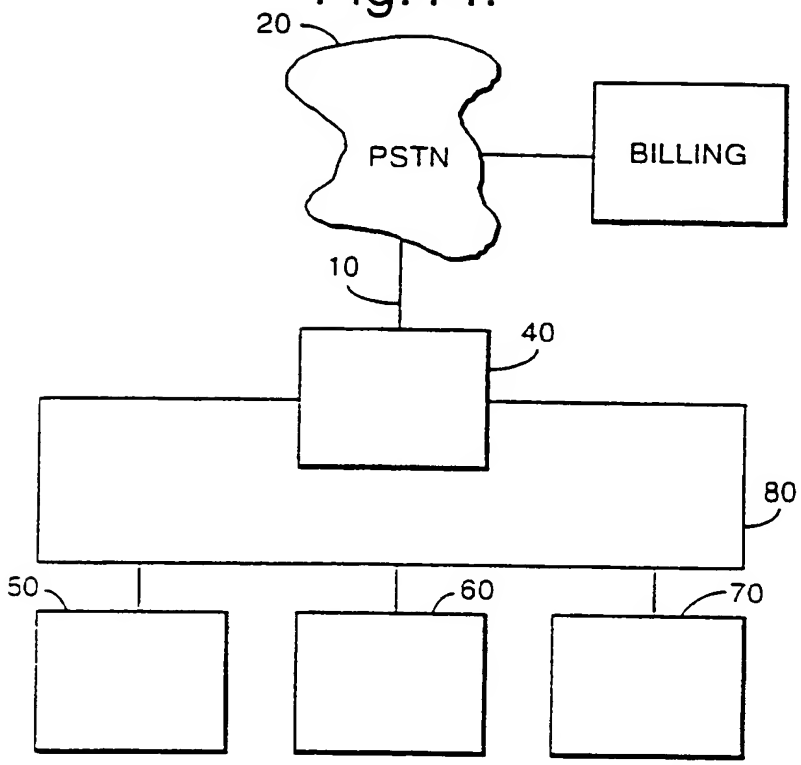


Fig.11c.



BNSDOCID: <WO_____9714085A1_I_>

Fig.14.



BNSDOCID: <WO_____9714085A1_I_>

INTERNATIONAL SEARCH REPORT

Int. onal Application No
PCT/GB 96/02489

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G06F1/00 G06F17/60 H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G06F H04L H04M G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO,A,93 01550 (INFOLOGIC SOFTWARE INC) 21 January 1993 see abstract see page 4, line 10 - page 5, line 5 see claims 1-8,23-31 ---	1-3,5,6, 8-17
Y	US,A,4 599 647 (GEORGE ASHOK K ET AL) 8 July 1986 see column 1, line 34 - column 2, line 65 see column 7, line 55 - line 61 see column 10, line 11 - column 11, line 53 ---	1-3,5,6, 8-17
A	US,A,5 325 419 (CONNOLLY DAVID A ET AL) 28 June 1994 see abstract see column 4, line 25 - column 5, line 49 see claim 1 --- -/--	8,10

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

1

Date of the actual completion of the international search	Date of mailing of the international search report
16 January 1997	23. 01. 97

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax (+31-70) 340-3016	Powell, D

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Inte. ›nal Application No
PCT/GB 96/02489

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO,A,84 01073 (KATZEFF KURT;PETRE TOMMY) 15 March 1984 see abstract	12-14
A	US,A,5 103 476 (WAITE DAVID P ET AL) 7 April 1992	
A	MAPPING NEW APPLICATIONS ONTO NEW TECHNOLOGIES, ZURICH, MAR. 8 - 10, 1988, no. -, 8 March 1988, PLATTNER B;GUNZBURGER P, pages 45-52, XP000215989 SIUDA K: "SECURITY SERVICES IN TELECOMMUNICATIONS NETWORKS"	
A	FR,A,2 697 358 (GENTRALP INTERNATIONAL BV) 29 April 1994	

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inte: ›nal Application No
PCT/GB 96/02489

Patent document cited in search report	Publication date	Patent family member(s)		Publication date
WO-A-9301550	21-01-93	AU-A-	2305292	11-02-93
US-A-4599647	08-07-86	NONE		
US-A-5325419	28-06-94	AU-A-	5985094	15-08-94
		CN-A-	1094882	09-11-94
		EP-A-	0678229	25-10-95
		JP-T-	8505743	18-06-96
		WO-A-	9416516	21-07-94
WO-A-8401073	15-03-84	SE-B-	432041	12-03-84
		AU-A-	2030183	29-03-84
		EP-A-	0138813	02-05-85
		US-A-	4577061	18-03-86
US-A-5103476	07-04-92	CA-A-	2095723	08-05-92
		EP-A-	0556305	25-08-93
		JP-B-	7089345	27-09-95
		JP-T-	6501120	27-01-94
		WO-A-	9209160	29-05-92
		US-A-	5222134	22-06-93
FR-A-2697358	29-04-94	NONE		

BNSDOCID: <WO_____9714085A1_I_>